Are You Ready For PCI v 3.0

Speaker: Corbin DelCarlo
Institution: McGladrey LLP
Date: October 6, 2014
Today’s Presenter

Corbin Del Carlo QSA, PA QSA
Director, National Leader PCI Services Practice
847.413.6319
Corbin.delcarlo@mcgladrey.com
Today’s Agenda

- How PCI compliance affects your institution
  - Processes and control modifications,
  - Breach concerns
- What is new to PCI V3.0
  - Requirements organizations struggle with
    - Challenges and myths
  - New requirements
  - Updated audit and evidence requirements
- The Future of PCI
  - Chip and PIN,
  - Mobile payments
  - Online transactions
How PCI Compliance Affects Your Institution
What is PCI DSS?

- Payment Card Industry Data Security Standard
  - An independent industry standards body providing oversight of the development and management of Payment Card Industry Security Standards
- Card brand members
  - American Express
  - Discover Financial
  - JCB International
  - MasterCard Worldwide
  - Visa, Inc.
- PCI Security Standards Council
  - Maintain PCI DSS standards and supporting documentation, and other PCI standards (i.e. PA DSS, PFI, etc)
Focus On The DSS

* Data Security Standard
  * Industry Standard for handling credit card data

* Expanded Guidance
  * Business-as-usual guidance
    * Compliance with the DSS is an ongoing process that businesses must keep up-to-date.
    * Security is not a point in time event
    * Adhering to the DSS on a daily basis, will have a positive effect on your business
How PCI Compliance Affects Your Business Processes

* **Costly Upgrades**
  * Network segmentation
  * Hardware and software upgrades
  * Vulnerability scanning
  * Monitoring and alerting systems
  * Fraud detection systems

* **Assessments and Attestations**
  * Implementing controls to protect cardholder data
  * Complete a report on compliance by a QSA (Qualified Security Assessor) or,
  * Perform a SAQ (self assessment questionnaire)
  * Attestation of Compliance (AOC)

* **Fines**
  * Not being PCI DSS compliant
Possible suggestions in making PCI DSS compliance run smoothly:

- Develop data flow diagrams
- Documentation of security policies, standards and operational procedures
- Create an inventory of your software and hardware that is in your cardholder data environment.
- PCI DSS is not an IT audit
  - Have key stakeholders available during an assessment.
  - Human resources, application owners, users of the applications, facilities, and IT specialist as needed to complete your PCI assessment.
Breach Concerns

* Hackers and large international organized crime syndicates
* Many small business owners
* Knowing what data you have and where it resides
* Higher monthly fees for non-compliance
* The fallout of a data breach
  * The fallout can be significant, including fines/penalties, termination of your ability to accept payment cards, lost customer confidence, legal costs, settlements and judgments, fraud losses, etc.
  * A breach could result a cost of, on average $200 per card number lost
* Key Themes
  
  * Education and awareness
    * Lack of education and awareness around payment security, coupled with poor implementation and maintenance of the PCI Standards, gives rise to many of the security breaches happening today.

  * Increased flexibility
    * Changes in PCI DSS and PA-DSS 3.0 focus on some of the most frequently seen risks that lead to incidents of cardholder data compromise—such as weak passwords and authentication methods, malware, and poor self-detection—providing added flexibility on ways to meet the requirements
What Is New To PCI V3.0
Differences: 2 Vs 3

* Total Changes – 89 modified requirements
  * Clarifications – added more specificity to the requirement language. Making the intent of the requirement more clear (74 changes)
  * Additional Guidance – providing further guidance or integrating supplemental documents released after v2 and integrating them into v3 (5 changes)
  * Evolving Requirement – changes to deal with the most recent threats and market changes. (10 changes)

* New Requirements – all fit into one of the above categories (16 new requirements)
Most of the changes in v3 were “clarifications” of the v2 requirements. (83%)

- Most of these were previously published via the Council’s FAQ website or the v2 Reporting instructions.

- These were already requirements
  - Wording just “codifies” the requirement

- Since this just indicate the intent of the existing requirement these are all technically required if you do version 2 or version 3
  - So hopefully you are already doing these.
Clarifications That Organizations Struggle With

- **E-Commerce Scoping Whitepaper**
  - Published in January 2013
  - Clarifies the scope of PCI DSS in relation to e-commerce apps
  - Most importantly pulls redirect systems into scope.

Images courtesy of PCI SSC
Information Supplement – PCI DSS E-Commerce Guidelines
eCommerce – Some Clarifications

- eCommerce – PCI Council
  - PCI_DSS_v2_eCommerce_Guidelines.pdf
  - Addresses multiple scenarios, including in-house, co-source, or out-source

- Clarification on out-source/re-direct
  - Merchant’s website redirects consumer’s browsers to an e-commerce payment processor’s website
  - Merchant is responsible for:
    - Managing website and servers (if self-hosted), including applicable PCI DSS requirements
    - Applicable PCI DSS requirements for managing third parties, (e.g., Requirement 12.8)
    - Having written agreements with any third parties and ensuring they protect cardholder data on behalf of the merchant, in accordance with PCI DSS.
    - Securing the web page(s) containing the redirection code and/or function(s).
Clarifications That Organizations Struggle With, continued

* Requirement 2.1 changing default passwords
  * Applies to all default passwords in the CDE.
  * Penetration tests still see default passwords most times.

* Requirement 3.4.1 disk encryption
  * Logical access must be managed separately and independently of the native operating system authentication and access control.
Clarifications That Organizations Struggle With, *continued*

- Requirement 6.4.1 separation environments
  - Prod and dev must be segregated by logical access controls
  - No developers have access to prod

- Requirement 10.2.1 Audit access to CHD
  - Requirement that all individual user access to CHD must be logged and included in the audit trails
  - No shared accounts without some other control
Clarifications That Organizations Struggle With, continued

* Requirement 10.6 daily log reviews
  * Clarified that log reviews should identify suspicious activity or anomalies
  * Allows risk management strategy to be applied to the logs reviewed
  * Actually a bit easier but almost requires a SIEM

* Requirement 12.8 Vendor Management
  * Clarified that the written service provider agreement/acknowledgement must document the responsibilities of the vendor in protecting CHD.
  * Much more detailed program will be required
New Requirements

* Scope of assessment
  * Evidence that card holder data only resides in the card holder data environment.
    * Proof via Data flow documentation
    * Interviews with business process owners
    * Automated scans at perimeter points

3.1 Assessor’s validation of scope accuracy

Document how the assessor validated the accuracy of the PCI DSS scope for the assessment, including:

- The methods or processes (for example, tools, observations, feedback, scans, data flow analysis) used to identify and document all existences of cardholder data.
- The methods or processes (for example, tools, observations, feedback, scans, data flow analysis) used to verify that no cardholder data exists outside of the CDE scope defined for this assessment.
- How the results of the methods/processes were evaluated to verify that PCI DSS scope is appropriate.
- How the results of the methods/processes were documented (for example, the results may be a diagram or an inventory of cardholder data locations).
- Why the methods used for scope verification are considered by the assessor to be effective and accurate.
- Provide the name of the assessor who attests that the scope of the assessment has been verified to be accurate and appropriate.
* Requirement 2.4 – Inventory of systems
  * Inventory was part of scoping before, not it is an actual requirement
  * Inventory will have to be very detailed
    * Include all system components that touch or support CHD processes
Requirement 5.1.2
- Protect all systems against malware
- Exception for systems that are not considered to be commonly affected by malicious software has been modified
  - Target Malware on POS
  - MacOS Safari Bugs
  - Android Malware
- Must be evaluated periodically (annually)

Requirement 6.5.10 – coding practices
* Coding protections have been updated to the new OWASP top ten
* Specifically added protections for:
  * Broken Authentication
  * Session management
* Requirement 8.5.1
  * Service Provider requirement for unique authentication for remote access at each customer premise
    * As a merchant this will have to be part of your acknowledgement/agreement

* Requirement 8.6 – unique token authentication
  * If using authentication such as physical tokens, smart cards, certificates, etc, the devices must be uniquely assigned
  * Each must only identify one user
    * Validate audit trail, provide non-repudiation
* **Requirement 9.9 – protect capture devices**
  * All devices that capture payment data (PIN PADs, Card swipes, CHIP readers, etc) must have unique tamper proof stickers
  * Periodic review of all stickers to validate not broken or substituted

* **Requirement 11.3 – Pentesting methodology**
  * Methodology has to be documented and based on industry standard (such as NIST SP800-115) and include current threats and vulnerabilities
  * Has to include the entire CDE and critical devices
  * Has to validate any segmentation or scope reduction controls used to reduce the scope of the assessment
  * Retention of remediation documentation.
* Requirement 11.5.1 – File Integrity Monitoring
  * Process must include responses to alerts generated.

* Requirement 12.8.5 – Vendor Management
  * Merchant must maintain information of which PCI DSS requirements are managed by each servicer provider or by the entity

* Requirement 12.9 – vendor acknowledgement
  * Service providers must provide and merchants must obtain written acknowledgement of responsibilities discussed in 12.8
Future Dated Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.10</td>
<td>Develop web applications to protect against broken authentication and session management</td>
</tr>
<tr>
<td>8.5.1</td>
<td><strong>Additional requirement for service providers:</strong> Service providers use a unique authentication credential for each customer</td>
</tr>
<tr>
<td>9.9</td>
<td>Protect card-reading devices used to capture payment card data from tampering and substitution</td>
</tr>
<tr>
<td>11.3*</td>
<td>Implement a methodology for penetration testing</td>
</tr>
<tr>
<td>12.9</td>
<td><strong>Additional requirement for service providers:</strong> Service providers acknowledge responsibility for the security of cardholder data (aligns with Requirement 12.8)</td>
</tr>
</tbody>
</table>

*PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place.*

*Effective July 1st, 2015*
The Future Of PCI
EMV – Chip And PIN

* EMV - Europay, MasterCard, and Visa.
* October 1, 2015 date for having EMV (Chip/PIN) implemented.
* Liability of loss shifts to merchant.
* Consider, however:
  * Are cards already encrypted?
  * Are they going directly from POS to processor and not entering the network?
  * What are the costs to implement POS?
  * Business perspective to update.
* Card Not Present (eComm, Mail In, Phone, Fax) not impacted.
* Confirm issuer and processor are ready for accepting Chip and PIN.
* Global Operations
  * Implement global, if not already done so.
  * Implement in US.
* P2PE – Point-to-Point Encryption – consider EMV as part of this solution.
* Multiple initiatives:
  * Some organizations are in process of implementing as part of POS upgrade tasks.
  * Some organizations are waiting to upgrade until it is time to replace POS devices.
  * Some organizations are waiting to see if the date is pushed back for EMV solutions.
  * EMV will likely move forward as a result of high rate of breaches. US does 24% of card transactions and is currently creating 47% of fraud activity.
Mobile Payments

* Mobile solutions are ok if they meet PCI requirements.
* PCI Council web site – February 2013
  Mobile_Payment_Security_Guidelines_Merchants_v1.pdf
* Additional guidance includes:
  * Mobile Payment-Acceptance Applications and PA-DSS FAQs
  * PCI PTS POI Modular Security Requirements, Version 3.1
  * PCI Payment Application Data Security Standard (PA-DSS), Version 2.0
  * Accepting Mobile Payments with a Smartphone or Tablet
* Risks:
  * Loss of mobile device could mean loss of payment information (physical security)
  * Capturing transmission of information
  * Securing the OS and checking for virus/malware
Mobile, continued

* Square solution or other type of external, approved reader or PED device.
* PA-DSS application that connects through mobile solution.
* P2PE solutions.
* Many trying to provide the market with a solution
  * Telecoms
  * Merchants
  * Processors
  * Software providers

Questions?